

US 60/177 304

corresponds to SE 99047 46-6

UNITED STATES PATENT APPLICATION

OF

CHRISTER FÄHRAEUS

AND

PETTER ERICSON

FOR

PAYMENT SYSTEM

Field of the Invention

The present invention relates to a payment product comprising at least one writing area which is intended for a user's signature and which is provided with a first position-coding pattern enabling digital recording of the signature, a system for electronic payment, a server unit for electronic payment, a use of a coding pattern, and a handheld electronic user unit.

Background

Security is a problem in connection with payments by check. There is always a risk that an unauthorized person will get hold of another person's checks, forge the person's signature, and in this way lay his hands on money which belongs to the owner of the check or buy goods with the check-owner's money.

Many solutions have been proposed which are aimed at making it more difficult for unauthorized persons to forge and use another person's checks.

EP 0 276 109 describes a check which, in a writing area where the user is supposed to write his signature, is provided with shading which varies in intensity from the top edge to the bottom edge. The user signs the check using a pen having a sensor which records the intensity at the point of the pen. The pen thus emits an output signal whose intensity varies over time depending on the position of the pen on the writing area.

As an alternative, the writing area can be provided with a large number of squares which all have shading of

varying intensity. In this case, too, the pen emits an output signal whose intensity varies over time depending on the position of the pen on the writing area.

The output signal from the pen can be used for comparing the user's signature with a previously stored signature for the user in order to ensure that it really is the authorized user who is signing the check in question.

Furthermore, there are problems associated with credit card payments. An unauthorized person who gets hold of another person's credit card can forge the credit card holder's signature on a credit card receipt and in this way buy goods with the credit card holder's money.

Another steadily increasing problem is security in connection with electronic payments via the Internet. One difficulty in this connection is the verification of the identity of a person who issues an electronic payment order.

Summary of the Invention

An object of the present invention is to provide a solution enabling increased security in connection with payment orders requiring a payer's signature.

This object is achieved by a payment product according to claim 1, a system for electronic payment according to claim 6, a server unit according to claim 16, a use according to claim 17, and a user unit according to claim 19.

More specifically, according to a first aspect, the invention relates to a payment product comprising

at least one writing area which is intended for a user's signature and which is provided with a first position-coding pattern enabling digital recording of the signature, the first position-coding pattern on the product being a subset of a larger, second position-coding pattern.

An advantage of using a position-coding pattern that is a subset of a larger position-coding pattern is that it is possible to increase security by using checks based on the knowledge that a specific payment product is provided with a specific subset of the larger position-coding pattern.

The first position-coding pattern on the product thus has a dual function. First, it enables the recording of a position of the pen, by means of which the signature is being written, locally on the writing area on the payment product. Secondly, it enables the determination of a position globally in the second, larger position-coding pattern, which position can be used for a security check.

An example of this is that various types of payment products, such as checks on the one hand, and bank giro forms on the other, can be provided with first position-coding patterns which constitute different subsets of the larger position-coding pattern. In order for a signature on a check to be accepted it is thus not sufficient for it to be similar to a previously stored signature as in the prior art, it must also be written on the "right" subset of the larger position-coding pattern. Further-

more, different payment products of the same type, such as checks with different numbers, can be provided with different subsets of the larger position-coding pattern.

The second, larger position-coding pattern need not be stored anywhere in its entirety. In this context, the fact the first position-coding pattern is a subset of a larger, second position-coding pattern means that the coding is such that additional unique first position-coding patterns can be created and that somewhere in a system where the payment product is utilized use is made of the fact that the position of the first position-coding pattern within the second position-coding pattern can be determined.

The payment product can have several writing areas, for example one writing area for stating an amount and another writing area for stating a payee or some other information which must be provided when a user is to make a payment. Advantageously, these writing areas can also be provided with a position-coding pattern so that the information written in these writing areas can also be recorded digitally. Preferably, it should be possible to provide a digital recording of all the information that is written on the payment product in connection with the payment. In this connection, the first position-coding pattern can be repeated in these writing areas or it can constitute a large part of the second, larger position-coding pattern in order to make it possible to distin-

guish between the positions within the different writing areas.

The larger position-coding pattern can, for example, consist of an image of an irregular object in which different partial areas or subsets with different appearances can be defined. However, the structure of the first position-coding pattern is preferably such that it codes coordinates for a plurality of points within a partial area on an imaginary surface. The advantage of this type of coding is that the second position-coding pattern need not be stored anywhere in its entirety; rather, it can be described by means of coordinates. Moreover, it is easier and less time-consuming to determine the position of the first position-coding pattern in the second position-coding pattern. In the above case involving an image, it is necessary to match the first position-coding pattern with different parts of the second position-coding pattern, which is time-consuming. Coordinates, on the other hand, provide a position immediately.

There are known position-coding patterns, see e.g. US 5,852,434, in which each position is coded with a unique symbol. This has the drawback that each symbol becomes fairly complex, at least if a large number of positions are to be coded, which in turn means that the symbols cannot be too small because then they will be difficult to read and the risk of error increases. Moreover, the device which is to read the position-coding pattern must read an area corresponding to four symbols

in each position in order to be certain to record a whole symbol. However, according to the invention, the first position-coding pattern is made up of a plurality of symbols, the coordinates of each point being coded with a plurality of symbols and each symbol contributing to the coding of more than one point. In this way, a high resolution is achieved. Examples of this type of code are provided in Applicant's Swedish patent applications SE 9901954-9 and SE 9903541-2 which were filed on 28 May 1999 and 1 October 1999 respectively. Said Swedish patent applications are herewith incorporated by reference.

In a particularly advantageous embodiment, the first position-coding pattern is unique to the authorized user of the payment product. Each user can thus be provided with his "own" subset of the larger position-coding pattern. This subset can, for example, be applied to the user's checks or to some other payment product belonging to the user, which he must sign in order to be able to use it. The user can, for example, be provided with personal credit card receipts which he signs when he wishes to make a payment using his credit card.

The fact that a payment product is provided with a position-coding pattern which is unique to the user considerably increases security since a fraudulent user must forge both a signature and a position-coding pattern.

Furthermore, this embodiment has the advantage that it becomes possible to use checks or other paper-based payment products for electronic payments. To date, a

user has been obliged to hand over a signed check made of paper when wishing to pay by check. Consequently, it has not been possible to use checks as a means of payment on the Internet. However, with a payment product according to present invention, it is possible to identify the payment product by reading the unique position-coding pattern upon which the signature is written and, consequently, it is possible to use the payment product to make electronic payments. In addition, this has the advantage that the user will have a paper copy of the payments he or she has made.

As mentioned above, the payment product can be any payment product which a user must sign in order to use it. For example, it can be a credit card receipt, a bank or postal giro form, or a voucher. In a preferred embodiment it is a check.

According to a second aspect, the invention relates to an electronic payment system, which system comprises a server unit, in which is stored data about a plurality of domains, each representing an area on an imaginary surface, and a plurality of user units, each of which is adapted to electronically record a signature of a user who wishes to make an electronic payment, the recording being made in the form of coordinates which are read from a payment product upon which the user writes his signature, and to transfer payment information comprising at least some of said coordinates to the server unit; the server unit being adapted, in response to receiving the

payment information from one of said user units, to identify the domain to which the coordinates belong.

Thus, according to the invention at least one imaginary surface is used which is divided into domains to enable secure electronic payment with the aid of payment products provided with coordinates. All the electronic payment orders in the system are channeled by the intermediary of a server unit which identifies the domain to which the coordinates, representing the user's signature, belong. The domains can be connected with payment products, with companies which in one way or another are associated with a payment order, or with users of a payment product which is signed by the user in connection with the payment. In this way it is possible to build one or several security levels into an electronic payment system. More specifically, the user's signature must be represented by coordinates associated with the "right" domain in order for the payment to be approved.

The system has many advantages for different users. An individual who is using the system can make secure electronic payments without using passwords, PIN codes, smart cards, or other security systems. Since the payment is recorded electronically, the user can keep her signed payment product as a reminder of the payment she has made.

A company that uses the system can rent a domain or gain access to it in some other way. Subsequently, the company can verify, or have the server unit verify, that

electronically recorded signatures are represented by coordinates from the right domain.

The coordinates recorded by the user units can be transferred to the server unit in a format requiring processing in order to enable the determination of the domain affiliation. They can also be transferred in explicit form.

As is evident from the above discussion, preferably at least one authorized user is associated with each domain and the server unit is adapted to verify the user's authorization with the aid of the domain affiliation.

A company can thus mark its payment products with coordinates associated with a certain domain. Before a user is authorized to use the payment product, the user must be registered with the company. Subsequently, the user can use the payment product and the company can make security checks by verifying that the user is in fact registered as an authorized user of the domain.

In an especially preferred embodiment of the system, which provides a high level of security, there is only one authorized user of a domain.

Moreover, in an advantageous embodiment, the server unit is adapted to compare the signature in the payment information from the user unit with a previously stored signature in order to verify the authorization of the user. The signature is represented in the form of coordinates received from the user unit. The coordinates thus

have the dual function of representing the signature as well as indicating the domain affiliation.

Furthermore, the user unit is preferably adapted to include a unique user identity, which is stored in the user unit, in the information to the server unit, the server unit being adapted to utilize the user identity for verifying the authorization of the user.

The user identity can be a production number of the user unit or some type of code which has been stored in the user unit specifically for this purpose.

The server unit can perform the entire verification of the payment information. However, the server unit is preferably only an intermediate unit which carries out some processing of the payment information received from the user units and subsequently forwards it to a receiver.

The receiver can be stated in the payment information, but in an advantageous embodiment, the receiver is determined by the domain affiliation. The receiver can be the party who rents or in some other way has the right to use the domain, for example a company, or some other receiver, whose address is associated with the domain.

The receiver can be a final receiver or an intermediate receiver who in turn forwards the information to the final receiver. The receiver can also be one of said user units, for example the user unit from which the server unit received the payment information.

The server unit can be adapted to include data about the domain affiliation in the payment information that is transferred to the receiver. The receiver can, for example, have the right to use a large domain or large number of small domains. The receiver may have provided users with payment products with unique position-coding patterns corresponding to a whole such domain or a part thereof. In that case, the receiver needs to know which domain or part thereof the payment information is associated with.

Furthermore, the server unit can be adapted to verify the authorization of the user with the aid of the domain affiliation and to include data about this in the payment information which is sent to the receiver. In this case, the server unit thus performs an additional part of the security check.

Another verification operation which advantageously can be carried out by the server unit is the verification of the authenticity of the user's signature. If so, data about the authenticity is included in the information to the receiver.

According to a third aspect of the invention, it relates to a use of a coding pattern on a payment product in order to enable the verification of whether the user is an authorized user of the payment product, the coding pattern being unique to the authorized user.

The advantage of this use is evident from the above discussion concerning the payment product and the payment system.

According to a fourth aspect of the invention, it relates to a server unit, which is adapted to form part of a system for electronic payment, the server unit having a memory in which is stored data concerning a plurality of domains, each representing an area on an imaginary surface, the server unit being adapted, in response to receiving the payment information which contains at least two coordinates, to identify the domain to which the coordinates belong.

The advantage of the server unit and further features of the server unit are evident from the above discussion. The operations of the server unit are preferably implemented with the aid of software.

According to a fifth aspect of the invention, it relates to a handheld electronic user unit, which is intended to be used in the above system.

In an advantageous embodiment, the holder's account number is stored in the user unit so that it can be transferred automatically to a server unit without the user having to record all the digits of the number on each occasion.

A handheld electronic user unit with at least one stored account number could be used in systems other than the one described above.

Brief Description of the Drawings

The present invention will now be described in more detail by way of exemplifying embodiments and with reference to the accompanying drawings, in which

Fig. 1 schematically shows a system according to an embodiment of the present invention;

Fig. 2 shows an example of a user unit; and

Fig. 3 schematically shows an example of a storage structure for storing, among other things, verification information in a server unit used for electronic processing.

Description of Preferred Embodiments

Fig. 1 shows an example of how a system according to the invention can be structured. The system generally comprises a plurality of payment products, a plurality of user units, a plurality of network connection units, and a server unit. However, for the sake of clarity, only one payment product 1, one user unit 2, one network connection unit 3, and one server unit 4 are shown in Fig. 1.

The Payment Product

The product 1 can be any type of payment product which can be provided with coordinates such that they can be read by the user unit. The coordinates can be stated either explicitly or in coded form.

In this example, the payment product 1 consists of a check which is provided with a position-coding pattern 5 across its entire surface. The pattern is shown very schematically and enlarged as a number of dots on the

check. The position-coding pattern 5 on the check constitutes a subset of a larger position-coding pattern.

The check has three writing areas 6a, 6b, 6c, which are intended for hand-written information. The first writing area is intended for an amount, the second writing area for a payee, and the third writing area for the user's signature.

The Position-coding Pattern

The position-coding pattern 5 has the characteristic that if an arbitrary part of the pattern of a certain smallest size is recorded, the position of this part in the position-coding pattern and thus on the payment product can be unambiguously determined.

The position-coding pattern 5 can be of the type shown in the above-mentioned US 5,852,434, where each position is coded with a specific symbol.

However, the position-coding pattern is advantageously of the type shown in Applicant's above-mentioned applications SE 9901954-9 and SE 9903541-2, where each position is coded with a plurality of symbols and each symbol contributes to the coding of several positions.

The position-coding pattern is made up of a small number of symbol types. One example is shown in SE 9901954-9, where a larger dot represents a "one" and a smaller dot represents a "zero". Another example is shown in SE 9901954-9, where four different displacements of a dot in relation to a raster point code four different values.

The User Unit

Fig. 2 shows an example of a user unit, which in this case consists of a digital pen. The pen comprises a casing 11 having approximately the same shape as a conventional pen. In one short side of the casing there is an opening 12. The short side is intended to abut against or be placed a short distance from the surface on which the position determination is to be carried out.

The casing 1 essentially contains an optics part, an electronic circuitry part, and a power supply.

The optics part comprises at least one light-emitting diode 13 for illuminating the surface which is to be imaged and a light-sensitive area sensor 14, such as a CCD or CMOS sensor, for recording a two-dimensional image. The user unit may also comprise a lens system.

The power supply to the user unit is obtained from a battery 15, which is mounted in a separate compartment in the casing.

The electronic circuitry part contains a processor 16 which is programmed to read an image from the sensor 14, to identify symbols in the image, to determine which two coordinates are coded by the symbols, and to store these coordinates in its memory. Furthermore, the processor 16 is programmed to analyze stored coordinate pairs and to transform them into a train of polygons which constitutes a description of the movement of the user unit across a surface provided with the position-coding pattern. Finally, the processor is programmed to generate

a message containing the train of polygons and a unique user identity which is stored in the user unit and to transfer this information to the server unit 4 by the intermediary of the transceiver 19 and the network connection unit 3.

The processor need not forward all the information to the server unit 4. The processor 16 can be programmed to analyze the recorded coordinates and only forward information represented by coordinates within a certain coordinate area.

The user unit also comprises a pen point 17, with the aid of which the user can write ordinary pigment-based writing which is simultaneously recorded by the user unit with the aid of the position-coding pattern. The pen point 17 is extendable and retractable so that the user can control whether or not it is to be used.

Moreover, the user unit comprises buttons 18 by means of which the user activates and controls the unit. It also comprises a transceiver 19 for wireless communication, for example by means of IR light or radio waves, with external units.

Communication with the Server Unit

The user unit is adapted to transfer payment information generated by the user to the server unit 4. In this example, the information is transferred by wireless means to the network connection unit 3, which in turn transfers the information to the server unit 4.

In this example, the network connection unit is a mobile telephone 3. Alternatively, it can be a computer or some other suitable unit having an interface to a network, for example the Internet or a local company network.

Alternatively, the network connection unit 3 can be integral with the user unit 2.

The communication between the user unit and the network connection unit, which are normally located fairly close to each other, can take place via IR or radio waves, for example according to the Bluetooth standard, or some other standard for information transfer over short distances. The transfer need not be wireless; rather, it can also be carried out by wire.

The Server Unit

The server unit is a computer in a computer network. It has the same structure as a conventional server unit with one or more processors, various kinds of memories, peripherals, and connections to other computers in the network, but it has new software for carrying out the operations described herein. It also has information stored in its memory to enable it to manage these operations.

All the user units are adapted to transfer their information to the server unit, which is thus a central unit in the system. However, several such systems put together can form an even larger system.

The server unit need not be part of a wide area network; rather it can be part of a local area network and be used for processing information, for example, within a company.

The Imaginary Surface

In the memory of the server unit is stored information about domains on at least one imaginary surface. The imaginary surface can be described as a surface in a coordinate system, which surface thus contains a large number of points that are systematically arranged in two dimensions with a certain given resolution. Each point can be defined by two coordinates. If there is more than one imaginary surface, more than two coordinates may be required to define a point.

On the imaginary surface there are a number of areas which can thus be described as domains. The domains can be of different sizes and shapes. The whole surface need not be covered with domains. Information about the different domains is stored in the server unit. A rectangular domain can, for example, be described with the aid of pairs of coordinates representing the points in the corners of the domain.

Rules

In a data structure in the memory of the server unit there is data or rules for each domain defining how the information associated with the domain should be processed.

Fig. 3 shows an example of such a structure, which in this case is a table. In a first column 30 in the table the domains on the imaginary surface are defined with the aid of the coordinates (x1,y1; x2,y2; x3,y3; x4,y4) for the corners of the domains, which in this case are assumed to be rectangular. A second column 32 defines a user of the domain, which in this case is bank A. A third column 32 defines a receiver of the information from the server unit. In this example, the bank is the receiver and, consequently, the third column states an e-mail address for the bank. A fourth column 33 defines an authorized user of the domain. In this example, Anders Andersson has checks with a position-coding pattern from the domain indicated in the first column. A representation of the authorized user's signature is stored in a fifth column 34, so that the server unit can compare a received signature with the previously stored signature. A sixth column 35 stores a user identity in the form of a serial number of the authorized user's user unit.

This is, of course, a very simplified structure which is only used to illustrate the principles. Much more complex structures and rules for the security check are conceivable.

Operation of the System

The operation of the system is as follows in this embodiment: With the aid of the pen point 17 of the user unit 2, a user writes an amount, a payee, and his signa-

ture on the check 1. The payment information is recorded electronically while it is being written by means of the pen point on the check by the user unit 2 continuously recording the part of the position-coding which is located within the field of view of the area sensor while the user is writing. The processor 16 transforms the position-coding pattern into coordinates. The processor thus generates a sequence of coordinates describing how the user has moved the user unit across the check while writing. The processor compresses the payment information by transforming it into a train of polygons. Subsequently, the processor generates a message containing the train of polygons and the unique user identity which is stored in the user unit. The message is transferred to the network connection unit 3 which in turn transfers the message to the server unit 4.

When the server unit 4 receives the message, it determines the domain to which one or several of the points in the train of polygons belong. Subsequently, it uses the rules associated with the domain for carrying out security checks.

Application Example 1

Suppose that the payment product is the check in Fig. 1. The user wishes to pay 1000 dollars to a company called Alfa using the check. The user writes the amount \$1000 in writing area 6a and the name of the company, Alfa, in writing area 6b. Subsequently, he signs the check in writing area 6c.

The user uses his personal user unit 2 for writing and signing the check, which unit records the payment information and includes this and the unique identity of the user unit in a message which is sent to the server unit. The server unit determines the domain to which the coordinates in the payment information belong. As described above with reference to Fig. 3, among other things, the name of the authorized user, the unique user identity of the authorized user's user unit, a previously stored signature of the authorized user, and the name of the receiver to which the payment information is to be transferred in a refined format are connected with this domain.

First, the server unit compares the signature in the payment information with the previously stored signature in column 34 in order to verify that the signatures match. Subsequently, the server unit compares the user identity in the payment information with the user identity associated with the domain in column 35 in order to verify that they also match. Furthermore, the server unit interprets the other payment information in the message and translates it into character-coded format. The character-coded payment information, the name of the user, and the result of the comparison is transferred to the receiver, which is the bank that has issued the check. If the user is the authorized user, the bank carries out the payment.

Alternatively, the server unit can be the bank's own server unit, which carries out the security check itself.

In the above example the position-coding pattern on the check is unique to the user. It can also be unique to each check so that the check number can be determined on the basis of the position-coding pattern. If so, the server unit can also verify that the check has not been used before and that it has a number that is consecutive to the previously used check. To further increase security, the position-coding pattern for the consecutive checks can be randomly distributed within a domain or belong to domains which are not consecutive.

Application Example 2

A credit card company has provided a user with a personal domain and a book of credit card receipts provided with the position-coding pattern from the domain. The position-coding pattern can be the same on all the receipts or different on each receipt if higher security is desired.

Suppose that the user finds a product on the Internet that he wishes to purchase. He will then be able to pay by using one of his credit card receipts and his personal user unit. He writes the amount payable, the payee, a reference, and any other information that is required to enable the payment to be identified on the credit card receipt, and signs the receipt.

The user unit includes the electronically recorded payment information in a message to the server unit and

supplements the information with the user's credit card number which is stored in the user unit.

The information is sent either to a server unit which carries out the same verifications as in the case of the check and sends a message with the payment information and the result of the authorization verification to the credit card company, or directly to the credit card company's server unit. As a further alternative, a first server unit to which the payment information is transferred can interpret the information and translate it into character-coded format and subsequently send the information to the credit card company, which is shown as the receiver of the information for the domain in question.

If instead the user is going to pay by credit card in a shop he can use one of his personal credit card receipts in the same way as described above, but instead he uses the shop's user unit when filling out the receipt and supplements the information with his credit card number which he writes on the receipt. In that case, the server unit will detect that the signature matches the previously stored signature for the user's personal domain, but that the unique user identity of the user unit does not match the one stated for the user's personal domain. The server unit can then check the user identity in a special table, whereupon it will find that it relates to a company user unit to which authorization information is to be returned. The shop will thus imme-

diately receive information stating that the payment is authorized and, moreover, the server unit will forward the payment information in the same way as described above.

What we claim and desire to secure by Letters Patent is:

1. A payment product comprising at least one writing area (6c) which is intended for a user's signature and which is provided with a first position-coding pattern (5) enabling digital recording of the signature, characterized in that the first position-coding pattern on the product is a subset of a larger, second position-coding pattern.

2. A payment product according to claim 1, wherein the first position-coding pattern (5) codes coordinates for a plurality of points within a partial area on an imaginary surface.

3. A payment product according to claim 1 or 2, wherein the first position-coding pattern is made up of a plurality of symbols (5a), the coordinates of each point being coded with a plurality of symbols and each symbol contributing to the coding of more than one point.

4. A payment product according to any one of the preceding claims, wherein the first position-coding pattern is unique to the authorized user.

5. A payment product according to any one of the preceding claims, which payment product is a check (1).

6. A system for electronic payment, which system comprises a server unit (4), in which is stored data about a plurality of domains, each representing an area on an imaginary surface, and a plurality of user units

(continued)

(continued claim 6)

(2), each of which is adapted to record a signature electronically for a user who wishes to make an electronic payment, the recording being carried out in the form of coordinates which are read from a payment product (1) upon which the user writes his signature, and to send payment information comprising at least some of said coordinates to the server unit (4); the server unit being adapted, in response to receiving the payment information from one of said user units, to identify the domain to which the coordinates belong.

7. A system according to claim 6, wherein at least one authorized user is associated with each domain and wherein the server unit (4) is adapted to verify the authorization of the user with the aid of the domain affiliation.

8. A system according to claim 6 or 7, wherein the server unit (4) is adapted to compare the signature in the payment information from the user unit (2) with a previously stored signature in order to verify the authorization of the user.

9. A system according to any one of claims 6-8, wherein the user unit (2) is adapted to include a unique user identity which is stored in the user unit in the information to the server unit (4) and wherein the server unit is adapted to use the unique user identity to verify the authorization of the user.

10. A system according to claim 6, wherein the server unit is adapted to forward the payment information to a receiver.

11. A system according to claim 10, wherein the receiver is determined by the domain affiliation.

12. A system according to claim 10 or 11, wherein server unit (4) is adapted to include information about the domain affiliation in the payment information which is sent to the receiver.

13. A system according to claim 10 or 11, wherein at least one authorized user is associated with each domain and wherein the server unit (4) is adapted to verify the authorization of the user with the aid of the domain affiliation and wherein the server unit is adapted to include data about the authorization of the user in the payment data which is sent to the receiver.

14. A system according to any one of claims 10-13, wherein the server unit (4) is adapted to compare the signature with a previously stored signature for the authorized user and to include data about the authenticity of the signature in the payment information which is sent to the receiver.

15. A system according to any one of claims 10-13, wherein the server unit (4) is adapted to verify the payment information by checking whether the user identity belongs to the authorized user of the payment product and to include information to this effect in the payment information.

16. A server unit, which is adapted to form part of a system for electronic payment,

the server unit (4) having a memory in which is stored data about a plurality of domains, each corresponding to an area on an imaginary surface, the server unit being adapted, in response to receiving payment information which contains at least two coordinates, to identify the domain to which the coordinates belong.

17. Use of a coding pattern on a payment product in order to enable the verification of whether the user is an authorized user of the payment product, wherein the coding pattern is unique to the authorized user.

18. Use according to claim 17, wherein the coding pattern is used for electronic recording of the user's signature.

19. A handheld electronic user unit, which is intended to be used in a system according to any one of claims 6-15.

20. A user unit according to claim 19, wherein an account number is stored.

Abstract of the Disclosure

A payment product has a writing area (6c) which is intended for a user's signature. In the writing area there is a first position-coding pattern (5) enabling digital recording of the signature. The first position-coding pattern is a subset of a larger, second position-coding pattern.

The payment product is used in a payment system, which is based on the transfer of electronic payment information recorded with the aid of the position-coding pattern to a server unit, which uses the position-coding pattern for verifying that the payment information is valid.

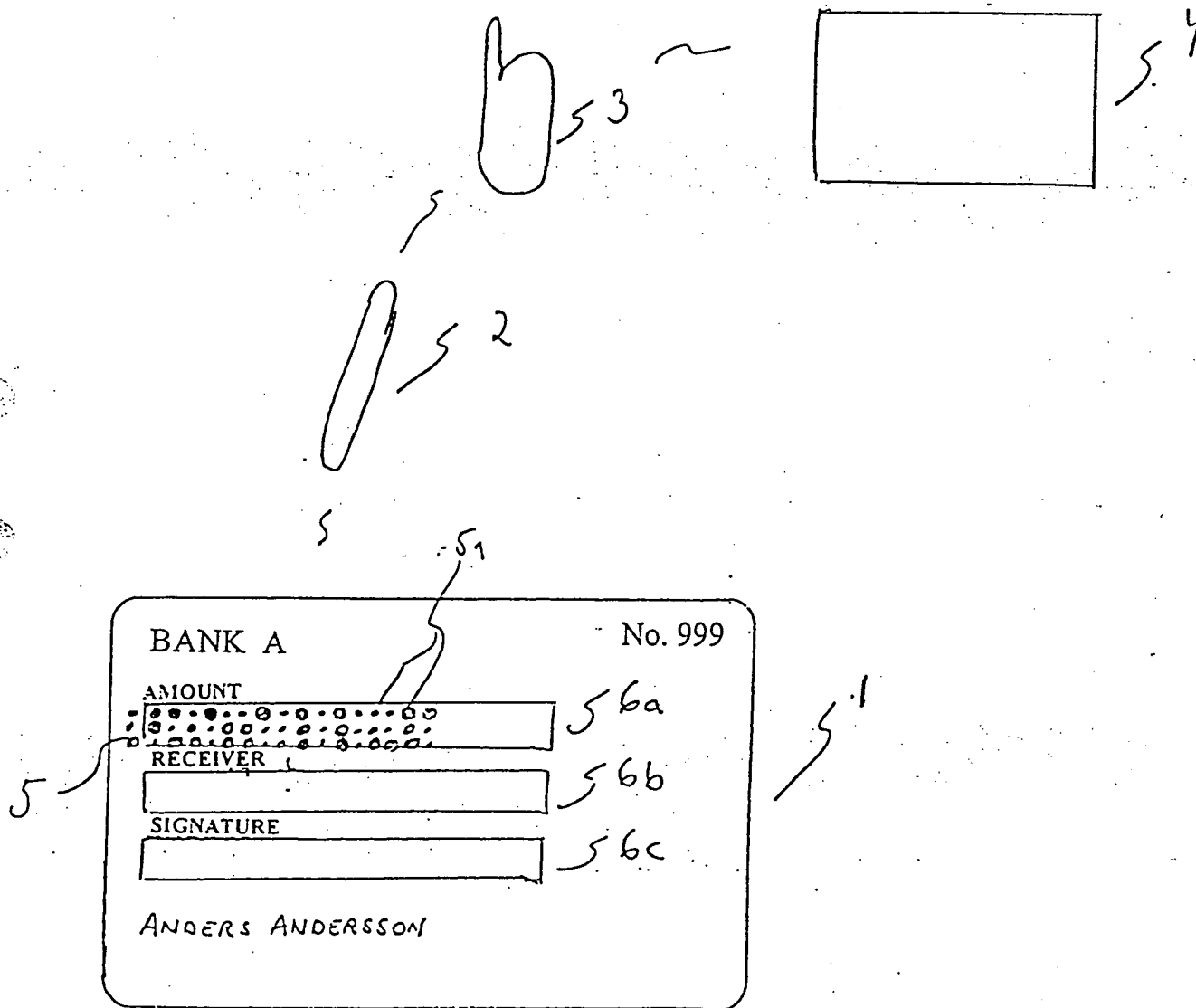


Fig. 1

30	31	32	33	34	35
DOMAIN	OWNER	RECEIVER	USER	SIGNATURE	USER IDENTITY
$(x_1, y_1); (x_2, y_2)$ $(x_3, y_3); (x_4, y_4)$	THE BANK A	BANK@SEK.SE	ANDERS ANDERSSON	<i>Anders Andersson</i>	123 456 789

Fig. 3

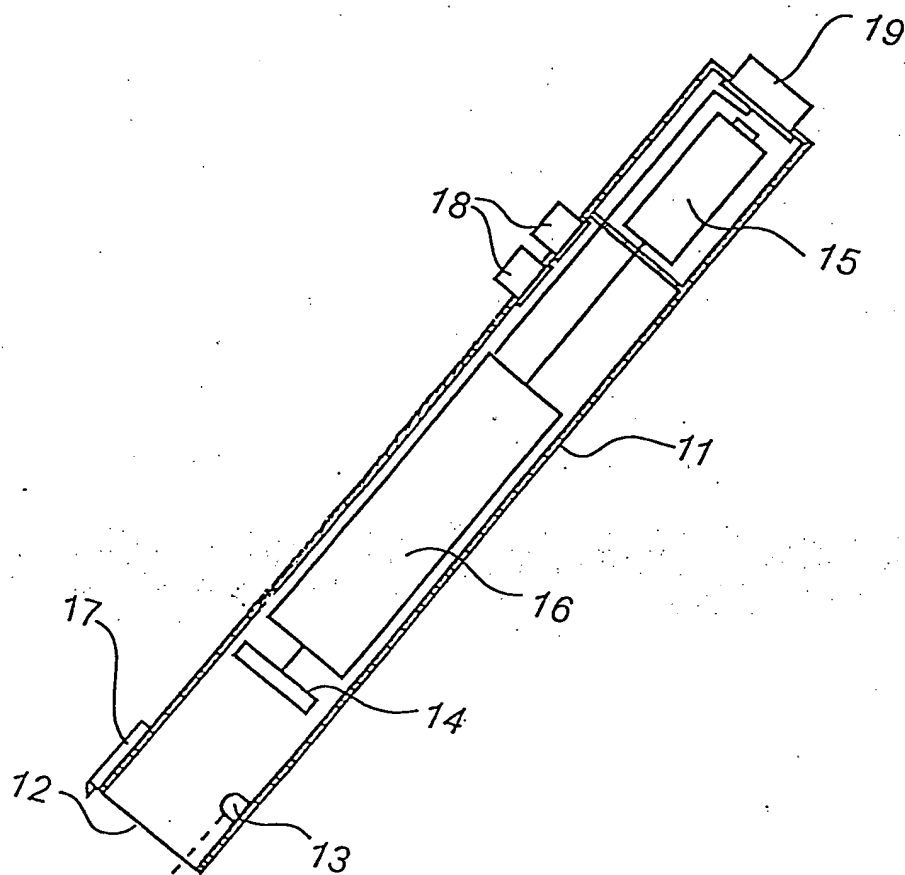


Fig. 2